UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information about the location of the cellular telephone assigned call number (312) 383-1405, as more fully described in Attachment A	)	Case No. 22-1840M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before 12/5/2022 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph .
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: 11/21/2022 @ 10:27 a.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

1. Records and information associated with the cellular device assigned call number **(312) 383-1405** (referred to herein and in Attachment B as "Target Cell Phone"), with listed subscriber unknown, that is in the custody or control of T-MOBILE, (referred to herein and in Attachment B as the "Provider"), a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, New Jersey, 07054.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

a. The following subscriber and historical information about the customers or subscribers associated with Target Cell Phone for the time period March 1, 2022, to the present:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records; and

ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by Target Cell Phone for the time period March 1, 2022, to the present including:

a. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

b. information regarding the cell tower and antenna face (also known as "sectors" through which the communications were sent and received), as well as PCMD, RTT, True Call, Advance Timing, NELOS, or equivalent data.

b. Information associated with each communication to and from Target Cell Phone for a period of **30** days from the date of this warrant, including:

i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;

ii. Source and destination telephone numbers;

iii. Date, time, and duration of communication; and

iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which Target Cell Phone will connect at the beginning and end of each communication, as well as PCMD, RTT, True Call, Advance Timing, NELOS, or equivalent.

c. Information about the location of Target Cell Phone for a period of 30 days during all times of day and night. "Information about the location of the Subject Phone" includes all available E-911 Phase II data, PCMD, RTT, True

Call, Advance Timing, NELOS, or equivalent, GPS data, latitude-longitude data, and other precise location information.

i. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the Provider, the Provider is required to disclose the Location Information to the government. In addition, the Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the Provider's services, including by initiating a signal to determine the location of Target Cell Phone on the Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Provider for reasonable expenses incurred in furnishing such facilities or assistance.

ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence of violations of Title 18, United States Code, Sections 1343 and 1346, involving NELSON FESINGHA.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this

electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information about the location of the cellular telephone assigned call number (312) 383-1405, as more fully described in Attachment A.

Case No.22-1840M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Sections 1343 and 1346	Wire Fraud and Conspiracy to commit wire fraud

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI SA Jennifer Peterson
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date 11/21/2022

Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jennifer L. Peterson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for the information about the location of the cellular telephone assigned call number **(312) 383-1405** ("**Target Cell Phone**"), whose service provider is T-Mobile ("Service Provider"), a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, New Jersey, 07054. The **Target Cell Phone** is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," see 18 Ulet me .S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. *See* 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. *See* 18 U.S.C. § 3123(b)(1).

3. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since December 2008. I am currently assigned to the Milwaukee Division – Green Bay Resident Agency. My duties as an Agent include investigating a variety of federal violations, to include but not limited to financial crimes such as wire fraud, money

laundering, and bank fraud. During my employment with the FBI, I have conducted several investigations that have resulted in seizures of criminally derived property, including monetary instruments and United States currency.

4. As a Special Agent, during the course of my investigations, I have used various investigative techniques, including conducting undercover operations, reviewing physical and electronic evidence, obtaining and reviewing financial records, and working with cooperating sources of information. I have also become familiar with techniques that criminals use to conceal the nature, source, location, ownership, and control of proceeds of crime and to avoid detection by law enforcement of their underlying acts and money laundering activities.

5. I am an investigator or law enforcement officer of the United States within the meaning of 18 U.S.C. Section 2510(7), in that I am empowered by law to conduct investigations of and to make arrests for federal felony offenses.

6. The facts in this affidavit come from my personal observations, training, experience, and information obtained from other agents, law enforcement officers, investigators, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your affiant has had regular contact regarding this investigation.

8. Based on the facts set forth in this affidavit, there is probable cause to believe that violations including, but not limited to, 18 U.S.C. §§ 1343 (wire fraud) and 1346 (conspiracy to commit wire fraud), are being committed, and will be committed by Durojuwa Omaghomi, NELSON FESINGHA, and others. There is also probable cause to believe that the location information described in Attachment B will constitute evidence of these criminal violations and will lead to the identification of individuals who are engaged in the commission of these offenses.

9. The court has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

10. The FBI, along with assistance from HSI and the Manitowoc County Sheriff's Office are investigating Durojuwa Omaghomi and NELSON FESINGHA's roles in a romance scam targeting elderly individuals throughout the United States. The investigation to date has revealed that one **Target Cell Phone** is used by FESINGHA, whose role in the scam is that of money mule, facilitating the transfer of victim funds to other individuals involved in coordinating the scam.

11. Romance scams are fraud schemes in which a perpetrator pretends to possess romantic intentions toward a victim to gain their affection. The perpetrator thereafter entices the victim to send money or merchandise on the perpetrator's behalf.

12. Romance scams are a lucrative way for criminals to steal money from vulnerable individuals, particularly in the elderly population. Victims are lured into the scams when perpetrators use aliases and stolen photographs to create online dating profiles and/or social media accounts. Generally, after grooming their victims, scammers create financial hardship scenarios necessitating requests for financial assistance.

13. The scammers enlist others to avoid detection by law enforcement and concerned family members of their victims. One role that others play is that of a "mule." A "mule" is a person who receives the fraudulently obtained money and merchandise on behalf of the scammer and subsequently forwards the proceeds to the scammer. A mule can be a witting participant, or a victim used to funnel proceeds to another mule.

Background on Omaghomi and FESINGHA

14. Omaghomi holds a valid California driver's license, is tied to several addresses primarily in Texas and California, and is connected to two businesses, Budzselect LLC and Shopbudz, with no legitimate business records or operations.

15. Based on records reviewed in this investigation, Budzselect LLC paystubs were created using a paystub creator website and subsequently used to substantiate a lease application in the name of Omaghomi for an apartment located at 5353 Las Colinas Blvd, Apartment 2105, Irving, TX 75039 (the "Texas Residence"). As detailed below, case agents believe that the apartment was leased by FESINGHA and that FESIGNHA is living there under Omaghomi's name.

16. FESINGHA's most current address is the Texas Residence. He has no valid driver's license.

17. Omaghomi has previously been convicted of possessing marijuana and driving while intoxicated in the state of Texas. FESINGHA was previously convicted of fraud, using/possessing identifying information in Texas, and traffic violations in Illinois.

18. Numerous financial reports have listed both Omaghomi and FESINGHA as the primary subjects associated with suspicious financial transactions. In 2015, both Omaghomi and FESINGHA were subjects of a money laundering and fraud investigation by the Slovak Republic. The Slovak Republic requested the assistance of the United States in locating and interviewing the subjects. It appears neither subject was located.

19. In the course of this investigation, I have interviewed several elderly victims and their family members. The victims have all sent money to names, addresses and/or businesses associated with Omaghomi.

20. The victims have all communicated in some fashion with individuals who have been identified as the scammers. Those scammers have been in contact with the **Target Cell Phone.** Omaghomi and FESINGHA are also in contact with several identified targets of other FBI investigations, primarily related to money laundering, business email compromises, and/or other fraud violations.

21. The investigation to date has revealed that the scammers contact victims, solicit business, convince victims to assist with paying work fines, or to help with travel back to the U.S. to be with the victims, to coordinate their scheme, and to facilitate fraud.

These scammers direct the victims where to send a specific amount of money, typically to residences or business associated with Omaghomi, but where FESINGHA has been physically observed.

22. One specific residence utilized is the Texas Residence. The lease applicant is listed as Omaghomi. The telephone number and email address listed on the lease application belong to FESINGHA. The apartment staff provided a statement that a man appearing to be FESINGHA, utilized Omaghomi's Texas driver's license, with a photo of FESINGHA, and completed the leasing paperwork.

23. Based on records obtained from USPS, UPS, and FedEx, over 20 packages, believed to contain checks or cash, were sent to addresses and/or aliases associated with Omaghomi. These include packages sent to: DUROJUWA OMAGHMI, DURO OMAG, DURO ORMA, and/or BUDZSELECT LLC. Victim statements corroborated that the money sent to these names/addresses were all under false pretenses. These victims believed they were in a romantic relationship and were sending money to help their "partner."

Victim 1

24. Victim 1, hereafter referred to as "AV1," a 75-year-old widow, with several health issues, believed she was in a relationship for several months with 'Richard Doolin,' utilizing a phone number that has also been in direct contact with **Target Cell Phone**. AV1 resides in Manitowoc, Wisconsin and lost over $250,000 due to this scheme.

25. In or around March of 2022, AV1 met 'Richard Doolin' on Facebook Dating and communicated several times a day via text messages, phone calls and an occasional email. AV1 considered her and Doolin in a relationship

26. AV1 believed Doolin to be the head contractor on an oil rig in the Gulf and he would be there until he retired. Doolin often mentioned visiting AV1 but then always managed to have an excuse of not being able to make it. Among the excuses he provided was that there was an issue with the oil rig and he was fined by OSHA.

27. As the relationship progressed, Doolin eventually asked AV1 to help him with some of the fines in hopes of getting home faster, to be with AV1. At Doolin's direction, in April of 2022, AV1 sent a $10,000 cashier's check to Budzselect LLC. The check was cashed at a Chase Bank located at 3183 Wilshire Blvd, Los Angeles, CA. Budzselect LLC is a company created by Omaghomi. It is also the company whose paystubs FESINGHA used to substantiate the lease application for the Texas Residence described above. The address of 3183 Wilshire Blvd., Los Angeles, CA, is also an address where Omaghomi resided (or currently resides).

28. In April and May of 2022, AV1 sent four checks totaling $198,000 payable to 'Hydra-Hose' in Tulsa, Oklahoma. This company belongs to Bonnie Masterson, a 74-year-old female, who was interviewed and is believed to be a money mule. Masterson's bank records illustrate this account was open strictly to receive fraudulent funds, which were all subsequently withdrawn in cash.

29. In May of 2022, AV1 sent $3,000 USD in cash to "Duro Omag" (an alias of Durojuwa Omaghomi) to 1501 Meridian Drive in Irving, Texas, Ave Las Colinas

Apartments. Management confirmed that Omaghomi resided at this address from 01/25/2021 to 04/24/2022 and that both Omaghomi and FESINGHA have been observed at this address. In June 2022, AV1 was instructed to send $20,000 concealed inside a teddy bear, to another victim, hereinafter known as "AV2".

30. On 08/16/2022, AV1 sent a package via USPS 1-day shipping with tracking #EI407231985US to be delivered to Irving, TX 75039. Utilize the tracking number on the USPS tracking website, delivery was confirmed on 08/17/2022 at 1509 hours to a parcel locker in Irving, TX. AV1 believed it was approx. $10,000 in U.S. currency that was asked to be sent to that address by the male on the phone for the purposes of getting a helicopter ride. IP address information was obtained by USPS pertaining to this tracking number and subpoena results provided the IP address tracking the package as the Texas Residence. On 08/17/2022 at approximately 1521 hours, an individual appearing to be FESINGHA, is captured on surveillance, picking up an envelope sent by a AV1.

31. In August of 2022, a package sent by AV1 and addressed to "Duro Omag" at the Texas Residence was intercepted by law enforcement. The package contained $30,000 in cash, hidden inside a teddy bear.

Victim 2

32. AV2 is an 81-year-old female residing in Ava, IL. AV2 was also part of the same romance scam. AV2 lost over $240,000 of her own money, but then received money from unknown individuals at the direction of the scammer and deposited the money in

her bank account. AV2 was instructed to send cash addressed to "Duro Omag" to the Texas Residence.

Victim 3

33. AV2 also received cash from Victim 3, hereinafter known as "AV3," a 73-year-old female residing in Youngsville, LA. AV3 was also part of the same romance scam. AV3 was directed to send at least five packages containing money to "Duro Omag," at the Texas Residence, one package to 1501 Meridian Drive, Apartment 2101, Irving, Texas, and at least one package to "Budzselect LLC" in Los Angeles, CA. AV3 lost over $312,000. The most recent number used to scam AV3, 765-276-3535, was in direct contact with the **Target Cell Phone** on at least two occasions.

Toll Records Analysis

34. A recent analysis of toll records for the **Target Cell Phone** from 01/01/2022 to 10/04/2022 identified a top contact as 312-613-6475, the main subject of a current FBI Business Email Compromise investigation. Approximately 30 contacts appear to be listed in 2022 escort ads, the majority in Texas.

35. **Target Cell Phone** and a phone number associated with Omaghomi have had approximately 275 exchanges with each other and have 20 common contacts.

36. On 10/28/2022, surveillance units in the vicinity of the Texas Residence, observed both FESINGHA and an individual they believed to be Omaghomi leave the apartment complex in a Chevy Malibu, with a temp tag, registering to FESINGHA. Omaghomi was driving and FESINGHA was the passenger.

37. Most recently, between 10/28/2022 and 11/02/2022, FESINGHA has had approximately 50 exchanges with 469-768-9434. Database records indicate the subscriber is Christopher Anekwe, residing at 6633 John Hickman Parkway, in Frisco, Texas. Anekwe is currently on probation/supervisory release for charges related to theft of government property, sale of stolen treasury checks, aiding and abetting, and aggravated identify theft. Surveillance teams have observed both FESINGHA and Omaghomi visit this address shortly after making phone contact with Anekwe. Two visits were observed for approximately 15-20 minutes.

38. The applied-for warrant seeks information on the **Target Cell Phone**, including cell-site location information that would reveal and corroborate witness accounts regarding FESINGHA's whereabouts during relevant events in this investigation. The locations would show, for example, whether FESINGHA was present in areas to which victims sent packages containing stolen funds. It would also help to demonstrate whether FESINGHA was in physical proximity to other targets. The location information would also show interstate travel from Los Angeles to Texas, and possibly Chicago, to continue exploiting elderly victims**.** In addition, the prospective information sought by this warrant would enable law enforcement to confirm where FESINGHA is currently residing.

39. Case agents and participants queried a law enforcement database to confirm the service provider of the **Target Cell Phone**. This query revealed that the service provider was T-Mobile Wireless. The **Target Cell Phone** subscriber is NELSON

FESINGHA, the subscriber since February of 2021, who provided an address of 4418 S. Indiana Ave., Chicago, IL 60653.

Cell-Site Data

40. In my training and experience, I have learned that the Service Provider is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the "sector" (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

41. Based on my training and experience, I know that T-MOBILE can also collect timing advance or engineering data commonly referred to as per call measurement data (PCMD, RTT, True Call, Advance Timing, Network Event Location Operating System Information (NELOS), or equivalent).

42. Based on my training and experience, I know that the Service Provider can collect cell-site data on a prospective basis about the Target Cell Phone. Based on my

training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as the Service Provider typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

E-911 Phase II / GPS Location Data

43. I know that some providers of cellular telephone service have technical capabilities that allow them to collect and generate E-911 Phase II data, also known as GPS data or latitude-longitude data. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. As discussed above, cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise than E-911 Phase II data. Based on my

training and experience, I know that the Service Provider can collect E-911 Phase II data about the location of the Target Cell Phone, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available.

Subscriber Information

44. Based on my training and experience, I know that wireless providers such as the Service Provider typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as the Service Provider typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the Target Cell Phone's user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST

45. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

46. I further request that the Court direct the Service Provider to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control.

47. I also request that the Court direct the Service Provider to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

48. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 180 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the Target Cell Phone would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. See 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible

property. See 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. See 18 U.S.C. § 3103a(b)(2).

49. Because the warrant will be served on the Service Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

CONCLUSION

50. Case agents believe that is reasonable to believe that the receipt of victim funds was generated by acts of mail fraud and wire fraud. As described above, the cellular information requested herein would facilitate further investigation of these criminal activities.

ATTACHMENT A

Property to Be Searched

1. Records and information associated with the cellular device assigned call number **(312) 383-1405** (referred to herein and in Attachment B as "Target Cell Phone"), with listed subscriber unknown, that is in the custody or control of T-MOBILE, (referred to herein and in Attachment B as the "Provider"), a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, New Jersey, 07054.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

a. The following subscriber and historical information about the customers or subscribers associated with Target Cell Phone for the time period March 1, 2022, to the present:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records; and

ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by Target Cell Phone for the time period March 1, 2022, to the present including:

a. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

b. information regarding the cell tower and antenna face (also known as "sectors" through which the communications were sent and received), as well as PCMD, RTT, True Call, Advance Timing, NELOS, or equivalent data.

b. Information associated with each communication to and from Target Cell Phone for a period of **30** days from the date of this warrant, including:

i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;

ii. Source and destination telephone numbers;

iii. Date, time, and duration of communication; and

iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which Target Cell Phone will connect at the beginning and end of each communication, as well as PCMD, RTT, True Call, Advance Timing, NELOS, or equivalent.

c. Information about the location of Target Cell Phone for a period of 30 days during all times of day and night. "Information about the location of the Subject Phone" includes all available E-911 Phase II data, PCMD, RTT, True

Call, Advance Timing, NELOS, or equivalent, GPS data, latitude-longitude data, and other precise location information.

i. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the Provider, the Provider is required to disclose the Location Information to the government. In addition, the Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the Provider's services, including by initiating a signal to determine the location of Target Cell Phone on the Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Provider for reasonable expenses incurred in furnishing such facilities or assistance.

ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence of violations of Title 18, United States Code, Sections 1343 and 1346, involving NELSON FESINGHA.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this

electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by T-MOBILE, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of T-MOBILE. The attached records consist of _____.

I further state that:

a. All records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of T-MOBILE and they were made by T-MOBILE as a regular practice; and

b. Such records were generated by T-MOBILE's electronic process or system that produces an accurate result, to wit:

1. The records were copied from electronic device(s), storage medium(s), or file(s) in the custody of T-MOBILE in a manner to ensure that they are true duplicates of the original records; and

2. The process or system is regularly verified by T-MOBILE and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature